APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

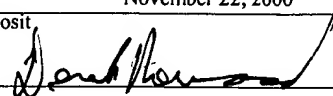APPLICANT: CARY A. JARDIN, ERIC VARSANYI, PHIL J. DUCLOS AND VINCENT M. PADUA

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No.   EL558603198US

I hereby certify under 37 CFR §1.10 that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

November 22, 2000
Date of Deposit

Signature

Derek Norwood
Typed or Printed Name of Person Signing Certificate

LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

TECHNICAL FIELD

This invention relates to securing information across networks, and more particularly to monitoring and controlling a link between a network device and a computer

5   for failures or intrusions.

BACKGROUND

The client/server model is often used to deliver information across a network. In this model, a client computer connects to a server on which information resides.

10   The client computer may request the services of the server, such as delivering information. Other services may include searching for and sending back information, such as when a database on a network is queried.

A conceptual diagram of a computer network 100, such

15   as the Internet, is illustrated in FIG. 1. The network 100 may comprise small computers 102-114 and large computers 120, 122, commonly used as servers. In general, small computers 102-114 are "personal computers" or workstations and are the sites at which a user operates the computer to

make requests for data from other computers or servers on the network 100.

A connection to the network 100 may be made through a network device 130-136 that provides an interface between the requesting computer (i.e. client) and the network infrastructure 140. The network device 130-136 may also be used to provide an interface between the network infrastructure 140 and the server 120, 122. The interface between the client 102-114, the server 120-122, and the network infrastructure 140 may be defined by a protocol referred to as the Hypertext Transfer Protocol (HTTP). The HTTP is the language that Web clients and servers use to communicate with each other. A secure version of this protocol, HTTP-S, is often used to provide communication between the network infrastructure 140 and the network device 130-136. However, the link between the network device 130-136 and the server 120-122, or the network device 130-136 and the small computer 102-114, is often configured in a non-secured mode.

DESCRIPTION OF DRAWINGS

These and other features and advantages of the invention will become more apparent upon reading the following detailed description and upon reference to the accompanying drawings.

5   Figure 1 is conceptual diagram of a computer network.

Figure 2 is a block diagram of a network system including a link lock system.

Figure 3 is a block diagram of a link lock system in accordance with an embodiment of the present disclosure.

10   FIG. 4 illustrates a method for monitoring and controlling a link for failures or intrusions according to an embodiment.

DETAILED DESCRIPTION

15   The present disclosure includes a link-lock system coupled to the network device to monitor and control the security mode of a link between the network device and the server or the client. The security mode of the link may be controlled in accordance with the status of the link. For

20   example, if a link failure or intrusion is detected, the security mode of the link is maintained in a secured state rather than converted into a non-secured state.

An embodiment of a network 200 having the link-lock system 206 is illustrated in FIG. 2. The network 200 includes a network interface device 204 configured to interface with the network infrastructure 201 through a link

5   202 operating in a secured protocol (e.g. HTTP-S). The HTTP-S provides a variety of security mechanisms to HTTP clients and servers, providing the security service options appropriate to wide range of potential end uses.

The network 200 further includes a link-lock system 206

10   coupled to the network interface device 204. The link-lock system 206 monitors security status of the link 208 between the network interface device 206 and a computer used to connect to the network, such as the server or the client 210. In the illustrated embodiment of FIG. 2, when the

15   link-lock system 206 determines that a link failure or intrusion is detected, the security protocol of the link 208 is maintained in an HTTP-S mode rather than converted into an HTTP mode. The link failure or intrusion may include physical tampering or alteration of any part of the link 208

20   between the network interface device 204 and the server/client 210. The failure or intrusion may also include software attack or modification of the link 208 from external sources.

A block diagram of the link-lock system 206 in

25   accordance with an embodiment of the present disclosure is

shown in FIG. 3. The link-lock system 206 includes a bus

monitor 300, a security switch 302, an encryption/decryption

element 304, and a controller 306. The link-lock system 206

may also maintain a protocol encryption element 308 on the

5 server/client 210.

The security switch 302 receives data from the network

interface device 204 or the server/client 210. In the

illustrated embodiment, the security switch 302 commands the

encryption/decryption element 304 to convert the received

10 data from a secured protocol to a non-secured protocol, when

the data is received from a network link 310 and is placed

onto the link 208. The security switch 302 may command the

encryption/decryption element 304 to convert the received

data from a non-secured protocol to a secured protocol, when

15 the data is received from the link 208 and is placed onto

the network link 310. The converted data is then sent to

the server/client 210 or the network interface device 204

using an appropriate protocol.

The bus monitor 300 monitors the link 208 for possible

20 link failure or intrusion. When a link failure or intrusion

is detected on the link 208, the bus monitor 300 notifies

the controller 306. The controller 306, upon receipt of the

link failure, directs the security switch 302 to keep the

link 208 in a secured protocol mode. The controller 306 may

25 also direct the protocol encryption element 308 in the

server/client 210 to convert the data being placed on the link 208 using a secured protocol. In some embodiments, the functions of the security switch 302, the bus monitor 300, and the controller 306 may be combined into a single

5 element.

FIG. 4 illustrates a method for monitoring and controlling a link for failures or intrusions. The method includes monitoring the link between a network device and a server/client, at 400. When failures or intrusions are

10 detected on the link, at 402, the link is directed to use a secured protocol at 404. Data sent across this link remains in a secured protocol mode until a network manager determines that the failures or intrusions have been corrected at 406.

15 Numerous variations and modifications of the invention will become readily apparent to those skilled in the art. Accordingly, the invention may be embodied in other specific forms without departing from its spirit or essential characteristics.